hetWaterschapshuis

De kracht van samen

Referentiearchitectuur voor cloud-gebaseerde IT-hosting

Definitief voorstel

Versie 0.9

30 juni 2022

Projectgroep Managed services

1 Management samenvatting 3

2 Inleiding 4

3 Architectuur IT-hosting 6
3.1 Componenten & eisen 6
3.2 Veiligheid 9

4 Bijlage: Dienst gebaseerd op de referentiearchitectuur 11
4.1 Waterschap Managed Service 11
4.2 WMS core services 11
4.3 WMS - infrastructuur 20
4.4 Service levels en service verzoeken 22

1 Management samenvatting

In dit document is een (referentie-)architectuur uitgewerkt voor cloud gebaseerde IT hosting.

Deze is opgesteld in het kader van het project Managed services, waarbij is onderzocht op welke wijze het mogelijk is om te komen tot de inrichting en gebruikmaking van clouddiensten voor cloud gebaseerde IT-infrastructuur voor hWh projecten. Deze architectuur is tevens bruikbaar voor waterschappen om hun inrichting vorm te geven en/of eisen te stellen aan derden voor de inrichting/ uitvoering van diensten m.b.t. de IT-infrastructuur.

Voor de uitwerking van een mogelijke implementatie wordt verwezen naar het document "Realisatiemogelijkheden Waterschap Managed services, op basis van de Referentiearchitectuur voor cloud-gebaseerde IT-hosting." Met dit laatste wordt de Referentie-architectuur bedoeld die in dit document is beschreven.

De reden om een dergelijke architectuur op te stellen is om te komen tot standaardisering van de inrichting van cloud-diensten op een zodanige manier dat beheersbaarheid, veiligheid en flexibiliteit gegarandeerd zijn.

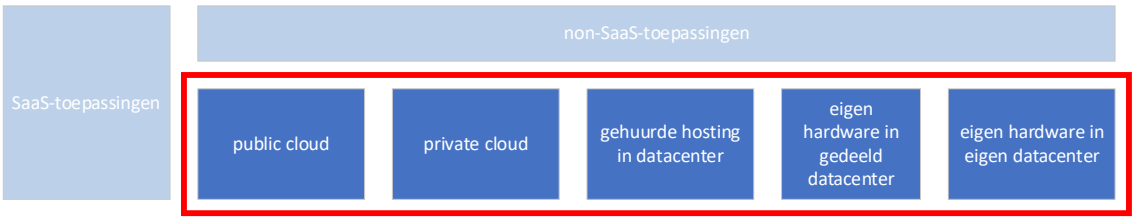
2 Inleiding

Alle waterschappen hebben (binnenkort) een Microsoft365 (M365) omgeving ingericht met daarin onder andere identity management ingericht op basis van Azure AD.

Voor alle toepassingen (applicaties, platformen, apps, etc.) is een grote verscheidenheid aan inrichtingen. Vanuit een hostingsperspectief is er allereerst een tweedeling te maken in SaaS en non-SaaS.

Van de SaaS-toepassingen ligt de verantwoordelijkheid voor de hosting volledig bij de leverancier en moeten de eisen van het waterschap contractueel geregeld zijn.

De non-SaaS-toepassingen kennen veel varianten in hostingsvormen, variërend van eigen hardware op een locatie van het waterschap, tot hosting bij een internationale cloud-leverancier.



Deze referentiearchitectuur helpt waterschappen bij inrichting van de hosting voor de non-SaaS-toepassingen. Hierbij is beschreven hoe een dergelijke omgeving veilig en robuust ingericht kan worden én hoe deze samenhangt met alle varianten van hosting die al aanwezig zijn.

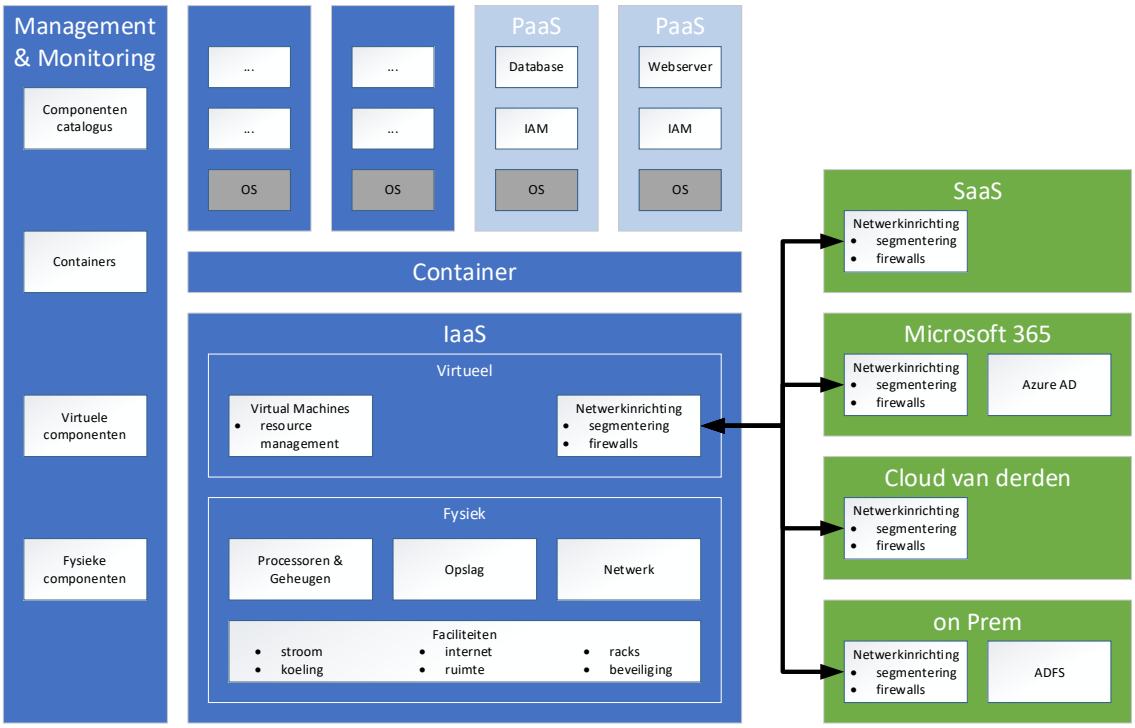
Deze referentiearchitectuur dient ook als basis voor een gezamenlijke hostingsdienst voor de waterschappen. Afhankelijk van de uitgangssituatie en ambitieniveau van ieder afzonderlijk waterschap, is er een specifieke implementatiestrategie per waterschap nodig.

In hoofdstuk ‘0

Architectuur IT-hosting' is beschreven hoe de architectuur is opgebouwd. In hoofdstuk '4 Bijlage: Dienst gebaseerd op de referentiearchitectuur', zijn de architectuurdelen gespecificeerd voor de dienst Waterschaps Managed Services (WMS) die op basis van deze architectuur wordt ontwikkeld.

3 Architectuur IT-hosting

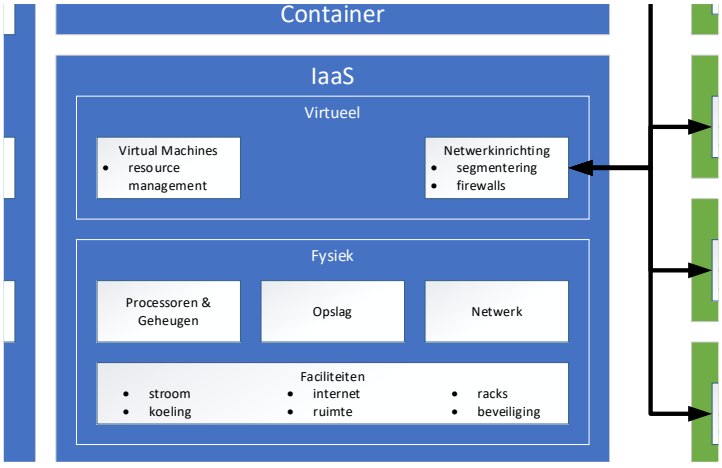
In onderstaande figuur is weergegeven uit welke onderdelen de WMS oplossing bestaat. Per onderdeel is kort weergegeven wat eronder verstaan wordt.



De groene blokken vormen geen onderdeel van de oplossing, maar zijn componenten (indien aanwezig) waarmee er wel afhankelijkheden zijn. Vaak zijn dit aanwezige voorzieningen die waterschappen in gebruik hebben. In volgende paragrafen is beschreven hoe de verschillende componenten functioneren en samenhangen

3.1 Componenten & eisen

3.1.1 IaaS



De basis van de dienstverlening is het aanbieden van de infrastructuur. Er worden virtuele machines (VM) geboden die onderling in een virtueel netwerk verbonden zijn. Deze machines

en dit netwerk bestaan uitsluitend softwarematig. Ze kunnen dus niet echt vastgepakt worden.

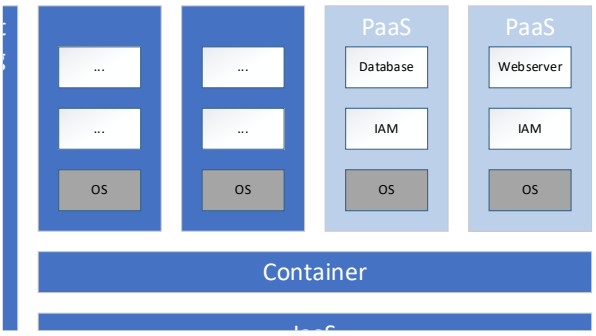
De virtuele componenten kunnen alleen bestaan als er ook een fysieke werkelijkheid is van processoren, memory, disk-ruimte en netwerkkabels die gedeeld worden door alle virtuele componenten. Om deze fysieke hardware goed te kunnen laten functioneren zijn er allerlei faciliteiten nodig, zoals een gebouw met stroom, internet, koeling.

Samen vormt dit een keten die zo sterk is als de zwakste schakel. Dit geldt voor allerlei aspecten, van beschikbaarheid tot veiligheid. Als in het fysieke gebouw de stroom of koeling uitvalt, vallen ook alle virtuele machines uit.

De virtuele infrastructuur kent meerdere beveiligingsmaatregelen. Toegang tot de systemen wordt op de netwerkverbinding direct verleend of geweigerd. De verschillende VM's staan alleen in een gedeeld netwerk als daar een technische noodzaak voor is. In andere gevallen zijn ze geïsoleerd van elkaar.

Het virtuele netwerk (software defined) is sterk gesegmenteerd. Alleen de noodzakelijke toegang tot een specifiek segment wordt gegeven en alleen noodzakelijke communicatie tussen specifieke segmenten wordt toegestaan. Hierdoor worden zowel de kans op, als de impact van bedreigingen, hacks, gijzeling, etc sterk gereduceerd.

3.1.2 Containers en meer



Omdat uitsluitend het bieden van infrastructuur in containers onvoldoende functionaliteit biedt om organisaties volledig te ontzorgen, zijn er ook platformen noodzakelijk.

Platformen bieden namelijk veel standaard functionaliteit waaraan op gebied van veiligheid wel scherpe eisen gesteld worden, maar waarbij de exacte inrichting voor de waterschappen van ondergeschikt belang is. Veilige platformen reduceren enorm de veiligheidsrisico's van de totale dienstverlening.

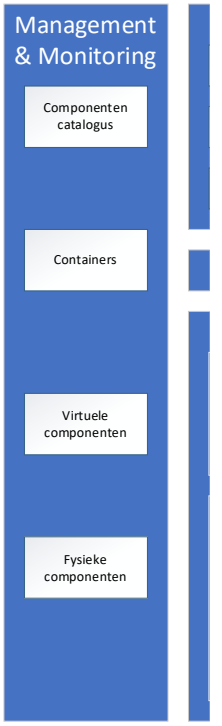
Door deze platformen centraal te managen kan het totale ICT-landschap sterk vereenvoudigd worden. Dit maakt niet alleen het onderhoud en beheer eenvoudiger en goedkoper, maar hierdoor kan er ook sneller opgetreden worden bij specifieke bedreigingen. Zo gauw een maatregel beschikbaar is voor één, is deze er ook voor allen.

De PaaS componenten draaien altijd in een container. Hiermee zijn ze gegarandeerd onafhankelijk van de onderliggende infrastructuur en is een verhuizing naar een andere omgeving of leverancier eenvoudig.

Platformen die nu al genoemd zijn:

- Webserver (IIS, Apache)
- Database (mogelijk meerdere varianten, Oracle, MySQL, Postgress)
- Applicatieserver
- API-management
- Low-code applicatieplatform

3.1.3 Management en Monitoring



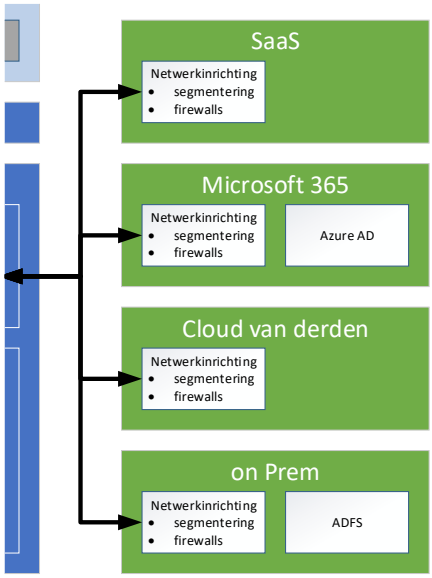
Ook de besturing en de monitoring van de omgevingen is sterk gestandaardiseerd. Het creëren van nieuwe onderdelen, het doen van onderhoud (patches, upgrades) en het op- en afschalen van resources, het creëren van netwerken en segmenten is allemaal gescript (software defined). De scripts kunnen ook via een portaal worden "afgetrapt". Hiermee ontstaat er 'Infrastructure as Code'.

De reden hiervoor is dat wijzigingen in de omgeving altijd traceerbaar en herhaalbaar zijn. Een bijkomend voordeel is, is dat individuele medewerkers zelf weinig of geen admin-rechten nodig hebben, dit voorkomt fouten door menselijke vergissingen én maakt de totale omgeving minder kwetsbaar. Vernieuwingen, verbeteringen en correcties zijn hierdoor direct toepasbaar voor alle systemen. De automatisering kost voor de eerste toepassing altijd meer tijd en geld, maar verdient zich op termijn altijd terug.

Bij het geautomatiseerd lanceren van een nieuwe omgeving wordt automatisch de logging en monitoring geregeld. Hierdoor is er geen enkel systeem dat ontsnapt aan de noodzakelijke controle en bewaking. Ook de inzet en gebruik van resources kan dan goed gemanaged worden (resource monitoring in combinatie met scale up en scale down), wat essentieel is voor een goede kostenbeheersing.

Essentieel voor het stimuleren van hergebruik is dat er een 'Componenten catalogus' is. In deze catalogus zijn alle componenten die als 'Infrastructure as Code' beschikbaar zijn eenvoudig vindbaar. Deze componenten kunnen direct "gelauncht" worden en zijn daarmee direct beschikbaar.

3.1.4 Interfaces



Vanuit de virtuele netwerkinrichting zijn beveiligde connecties mogelijk met:

- Microsoft 365 (als de IaaS onder de Enterprise Agreement afgenomen wordt van Microsoft, zal dit in dezelfde omgeving zitten)
- SaaS-diensten
- Andere cloud-diensten
- On-Prem datacenters

Deze verbindingen zijn, net als het interne netwerk, gescript. Hierdoor is standaardisatie en veiligheid goed te garanderen.

Voor de verschillende connecties worden standaarden gedefinieerd (inrichting van switches, firewalls, etc.) die door scripts afgedwongen worden.

3.1.5 Standaarden -2

Omdat standaardisatie de sleutel tot succes is voor zowel de kostenbeheersing als de veiligheid, wordt het aantal varianten van iedere platform sterk beperkt.

Van iedere standaard worden drie versies ondersteund, de laatste tot en met de twee-na-laatste (n-2). Hierdoor heeft iedere gebruiker van de dienst voldoende tijd om bij een nieuwe versie de overstap te maken. Dit moet dan gebeurd zijn vóór de volgende nieuwe versie (+1) beschikbaar komt. Door deze versies hard af te dwingen, wordt voorkomen dat er onderdelen in de omgeving achter gaan lopen en daarmee risico's lopen in veiligheid en support.

3.2 Veiligheid

De veiligheid is op alle niveaus van de dienstverlening 'by design' geregeld. De veiligheid wordt continu gemonitord en periodiek getest. De architectuur moet voldoen aan de eisen die vanuit de verschillende baselines, classificaties en richtlijnen vanuit de overheid worden gesteld, waaronder de richtlijnen van de Baseline Informatiebeveiliging Overheid (BIO) en deze richtlijnen worden als basis van hun security inrichting gebruikt.

Voor de inzet van cloud-oplossingen worden de richtlijnen gevolgd zoals omschreven door het Nationaal Cyber Security Center (NCSC) in "ICT-Beveiligingsrichtlijnen voor Webapplicaties" en "Factsheet: 5 adviezen voor veilig inkopen van clouddiensten" en NIST SP 1800-19 Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments.

Bij iedere realisatie van deze architectuur moet het technische detailontwerp aan deze richtlijnen getoetst worden. Ook de feitelijke implementatie moet periodiek getoetst worden of deze (nog) compliant is aan de richtlijnen.

3.2.1 Fysiek

Uitsluitend geautoriseerd personeel heeft toegang tot de fysieke hardware. Voorzieningen als stroom, netwerk en koeling zijn hoog beschikbaar. Waar nodig is de dienst op meerdere, geografische gespreide, locaties beschikbaar.

3.2.2 Netwerken

Intern is het netwerk gesegmenteerd waarbij er alleen specifieke type verbindingen mogelijk zijn tussen segmenten waarvoor dat expliciet is toegestaan. Dit wordt afgedwongen met Network Access Control (NAC) en zorgt voor netwerk boundaries door gebruik van dedicated virtual local area networks (VLANs) en automated access control lists (ACLs) Verbindingen met externe resources gaan altijd via beveiligde VPN-verbindingen. Wijzigingen in de netwerken en firewalls kunnen uitsluitend door management-accounts worden aangebracht, waarbij er expliciete controle is op de scripts die door deze accounts worden uitgevoerd. Zogenaamde named-users kunnen hooguit scripts aanmaken. Doormiddel van 'immutable logs' is altijd te detecteren wie welke wijziging heeft geïnitieerd.

3.2.3 Machines

Wijzigingen in de machines kunnen uitsluitend door management-accounts worden aangebracht, waarbij er expliciete controle is op de scripts die door deze accounts worden uitgevoerd. Hierdoor is er een beperkte groep van accounts die kritische wijzigingen kunnen doorvoeren. Deze groep wordt zwaarder gemonitord om misbruik te voorkomen en snel te detecteren (Privileged Identity Management, PIM). Zogenaamde named-users kunnen hooguit scripts aanmaken. Doormiddel van 'immutable logs' is altijd te detecteren wie welke wijziging heeft geïnitieerd.

3.2.4 Platformen

Platformen bieden maar een beperkt aantal alternatieven aan (standaarden -2). Hierdoor is bij geconstateerde bedreigingen of lekken, de impact snel duidelijk. Maatregelen (patches of desnoods uitzetten) kunnen snel doorgevoerd worden. Wijzigingen in de platformen kunnen uitsluitend door management-accounts worden aangebracht, waarbij er expliciete controle is op de scripts die door deze accounts worden uitgevoerd. Zogenaamde named-users kunnen hooguit scripts aanmaken. Doormiddel van 'immutable logs' is altijd te detecteren wie welke wijziging heeft geïnitieerd.

3.2.5 Toepassingen

Gebruikers worden geïdentificeerd en geauthentiseerd met behulp van Azure AD. Dit is de Azure AD van de eigen organisatie. Als de IaaS door Microsoft wordt geleverd is dit een "interne" dienst. In andere gevallen wordt er een SSO-verzoek gestuurd naar de Azure AD van de organisatie.

3.2.6 Privacy-eisen

De privacy van de gebruikers is gegarandeerd doordat de oplossing geen eigen registratie van persoonsgegevens van gebruikers bijhoudt, maar altijd gebruik maakt van de identificatie en authenticatie van Azure AD.

Over de privacy-eisen van de gegevens die in de toepassingen verwerkt worden, kan in algemene zin niets gezegd worden. Dit hangt volledig af van de goede inrichting van de applicatie zelf. De omgeving biedt wel alle technische mogelijkheden die nodig kunnen zijn.

4 Bijlage: Dienst gebaseerd op de referentiearchitectuur

Als er gebaseerd op deze referentiearchitectuur een dienst voor een of meerdere organisaties (waterschappen, hWh, UvW, …) wordt ingericht, ontstaan er specifieke aanvulling op de referentiearchtiectuur

4.1 Waterschap Managed Service

Waterschap Managed Service (WMS) is een standaard en schaalbare hosting oplossing.

WMS biedt computerverwerkings-, opslag- en back-updiensten op een flexibele manier. Er wordt een passende beveiligde netwerkverbinding gerealiseerd, waardoor de waterschappen toegang hebben tot de diensten

De computercapaciteit bevindt zich in het datacenter van een leverancier. Waterschappen hebben een gelimiteerd aantal keuzes voor het besturingssysteem van de virtuele servers (Microsoft Windows-, Red Hat Linux). Elke waterschap omgeving heeft zijn eigen afzonderlijke beveiligingszone(s). Deze omgeving is toegankelijk via een beveiligde verbinding via internet of een speciale WAN-verbinding.

Er zijn twee servicevarianten van WMS voorzien, 'managed' en 'unmanaged'. In beide varianten wordt een omgeving (besturingssystem, rekencapaciteit, geheugen, opslag en backup) geleverd. Het verschil in dienstverlening zit in het beheer van de omgeving.

Unmanaged omgevingen zijn bedoeld voor tijdelijke, experimentele toepassingen zoals PoC's, sandboxes, etc. Monitoring en patches zijn niet beschikbaar, de omgevingen zijn volledig geïsoleerd van de managed omgevingen en de omgeving wordt na een afgesproken tijd verwijderd. Veel van de dienstverlening die in 4.2 is beschreven is dus **niet** van toepassing.

WMS is een gestandaardiseerde oplossing en wordt standaard gehouden om efficiënt de benodigde functionaliteit mogelijk te maken en te behouden. WMS ondersteunt alleen n-2 versies. Zowel de waterschappen en de leverancier van de WMS moeten acties ondernemen om in een ondersteunde configuratie te blijven.

WMS bestaat uit de volgende modules:

- Platform en provisioning
- Levenscyclusbeheer
- Opslag- en gegevensbeschermingsdiensten
- Incident & Change management
- Data backup en recovery
- WAN Services
- Applicatie blueprinting
- Disaster recovery

4.2 WMS core services

WMS verplichte diensten bestaan uit een reeks gemeenschappelijke standaarddiensten over de infrastructuurcomponenten.

4.2.1 Infrastructuur management

Infrastructuur management verwijst naar de hardwarecomponenten voor WMS en hun werking, bestaande uit de volgende componenten:

1. Infrastructuur operatie

Infrastructuuractiviteiten bestaan uit het leveren, repareren of vervangen van de WMS-infrastructuurcomponenten om te voldoen aan de servicebeschikbaarheidsdoelen.

Leverancier zal voldoen aan de verantwoordelijkheden zoals uiteengezet in de volgende tabel.

No.	Taak
1.	Maak support overeenkomst met de hardware vendors.
2.	Administratie hardware systeem compute, network, storage en backup.
3.	Coordinatie hardwarecomponenten vervangingen en/of patching met vendor ondersteuning.
4.	Leg vast en update de hardware asset inventaris voor de WMS-dienst.
5.	Initieer het proces om hardware systeem capaciteit te implementeren, als overeengekomen met het Waterschap.
6.	Ontvang capaciteits drempel waarschuwingen, bewaak capaciteitstrend statistieken en breng het waterschap op de hoogte van capaciteitsproblemen.
7.	In geval van een hardwarestoring binnen de WMS-dienst zal de defecte hardware worden vervangen door de leverancier.
8.	Monitoring van de hardware infrastructuur.

2. Infrastructuur uitbreiding

Infrastructuuruitbreiding bestaat uit de installatietaken die nodig zijn om de extra vereiste componenten toe te voegen aan de WMS-infrastructuuronderdelen.

Leverancier zal zich houden aan de verantwoordelijkheden, zoals uiteengezet in de volgende tabel.

No.	Taak
1	Aanschaf extra server/storage/netwerk set of levering uit een bestaande voorraad.
2	Beheer de commerciële overeenkomsten en logistiek met de geselecteerde hardwareleveranciers.
3	Bewaak de levering van de hardwarecomponenten volgens de overeengekomen klantenserviceniveaus voor het leveren van de extra capaciteit die door de extra hardware wordt geboden.
4	Installeer de compute rack/node set in het aangewezen WMS-infrastructuuronderdeel volgens het standaard leverancier ontwerp en de benodigde beveiligings basisregels.
5	Configureer de WMS-infrastructuurcomponent om op softwareniveau de nieuwe hardware te beschikbaar te maken.
6	De configuratie database (CMDB) en rapportage bijwerken om de nieuwe toegevoegde hardware weer te geven.
7	Werk de onderhoudsdocumentatie bij met de nieuwe hardware details.
8	Voeg de nieuwe hardwaredetails toe aan de patchschema's.
9	Informeer Waterschap / gebruikersorganisatie wanneer alle taken in deze sectie zijn voltooid.

3. Opslagbeheer

Opslagbeheer bestaat uit de activiteiten die nodig zijn om de opslag voor de WMS-infrastructuur te beheren.

Leverancier zal zich houden aan de verantwoordelijkheden, zoals uiteengezet in de volgende tabel.

No.	Taak
1.	De Opslagklasse toewijzen/verwijderen/configureren binnen het WMS
2.	Bewaak de opslagcapaciteit van WMS-opslag.
3.	De prestaties van het opslagsubsysteem bewaken.
4.	Geef prognoses over toekomstige opslagvereisten

4. Netwerk
[todo]

4.2.2 Beschikbaarheid management

Leverancier zal voldoen aan de verantwoordelijkheden, zoals uiteengezet in de volgende tabel.

No.	Taak
1.	Activiteiten uitvoeren ter ondersteuning van de levering volgens de beschikbaarheids- en serviceniveaudoelen.
2.	Beschikbaarheids monitoring en -rapportage onderhouden.
3.	Monitoren om incidenten te voorkomen en op te sporen.
4.	Proactief beheer om ongeplande uitval mogelijk te verminderen.
5.	Activeer het incident proces automatisch, indien nodig.
6.	Gebruik role-based access voor beschikbaarheids management.

4.2.3 Servicemanagement

Servicebeheer bestaat uit de taken die nodig zijn om te voldoen aan de infrastructuur gerelateerde serviceniveau doelen die nodig zijn om WMS te beheren en om provisioning- en serviceaanvragen te ondersteunen.

Leverancier zal zich houden aan de verantwoordelijkheden, zoals uiteengezet in de volgende tabel.

No.	Taak
1.	Leveren servicemanagement en administratie van de WMS-management software.
2.	Integreer de WMS-service met het servicemanagement framework van het waterschap.
3.	Patch- en onderhoudsactiviteiten uitvoeren, in overeenstemming met het beveiligingsbeleid en de richtlijnen van het waterschap.
4.	Leverancier in staat te stellen geplande patch- en onderhoudsactiviteiten uit te voeren binnen de overeengekomen onderhoudsvensters en eventuele ongeplande patch- en onderhoudsactiviteiten, in overeenstemming met de serviceniveaudoelen.
5.	Lever alle operatie supportactiviteiten voor de WMS service.
6.	Registreer en update de software asset en licentie inventaris voor de WMS-service.
7.	Coördineer softwareondersteuning met de leverancier(s).
8.	Gebruik role-based access voor service management.

4.2.4 Virtuele server management

Virtueel serverbeheer bestaat uit activiteiten met betrekking tot de software en hardware in de compute services binnen de WMS-service.

Compute Services biedt een pool van virtuele CPU, geheugen en een bibliotheek met verschillende virtuele servergroottes van waaruit het waterschap zijn eigen virtuele servers kan maken.

Virtuele servers bestaan uit de volgende onderdelen:

1. Productiesupport, virtuele servers (managed)
   Productieondersteuning, fysieke servers ondersteunen de omgeving waarin de virtuele servers worden uitgevoerd, indien gekozen tot en met het besturingssysteem.

   Waterschap en Leverancier zullen voldoen aan de verantwoordelijkheden, zoals uiteengezet in de volgende tabel.

No.	Taak	Leverancier	Waterschap
1.	Registreer virtuele servers in WMS management stack.	X	
2.	Geautomatiseerde activiteiten van WMS-beheerstacks voor servers beschikbaar.	X	
3.	Beheer van administratie- en beheeraccounts die door het waterschap zijn overhandigd.	X	
4.	Beheer- en beheeraccounts die aan het waterschap zijn gekoppeld om deze accounts aan echte personen te koppelen. (Geanonimiseerde of echte accounts).		X
5.	Accepteer dat logboeken worden opgeslagen om administratieve activiteiten bij te houden.		X
5.	Beheer de hypervisors die de virtuele servers van de WMS leveren.	X	
6.	Beheer de virtuele servers, in overeenstemming met de beveiligingsrichtlijnen van het waterschap.	X	
7.	Bewaak de hypervisors en hosts van de WMS op de beschikbaarheid en capaciteit van systeemgebeurtenissen.	X	
8.	Waterschap op de hoogte stellen in geval van problemen.	X	
9.	Aanvragen voor nieuwe virtuele server(s) of wijzigingen in bestaande virtuele server(s) initiëren als standaard serviceverzoek.		X
10.	Alle standaard serviceaanvragen verwerken, in overeenstemming met de serviceniveaudoelen	X	
11.	Incidentbeheer uitvoeren op problemen die worden veroorzaakt door gebeurtenissen en/of waterschap.	X	
12.	Wijzigingsbeheer uitvoeren voor alle aanpassingen die nodig zijn om de omgeving van de virtuele servers te onderhouden volgens de serviceniveaudoelen	X	
13.	Gebruik role-based access voor productiesupport.	X	

2. Ontwikkelsupport, virtuele servers (unmanaged)
   Ontwikkelondersteuning, virtuele servers zonder ondersteuning

Waterschap en Leverancier zullen voldoen aan de verantwoordelijkheden, zoals uiteengezet in de volgende tabel.

No.	Taak	Leverancier	Waterschap
1.	Registreer virtuele servers in WMS management stack.	X	
2.	Geautomatiseerde activiteiten van WMS-beheerstacks voor servers beschikbaar.	X	
3.	Beheer van administratie- en beheeraccounts die door het waterschap zijn overhandigd.	X	
4.	Beheer- en beheeraccounts die aan het waterschap zijn gekoppeld om deze accounts aan echte personen te koppelen. (Geanonimiseerde of echte accounts).		X
5.	Accepteer dat logboeken worden opgeslagen om administratieve activiteiten bij te houden.		X
5.	Beheer de hypervisors die de virtuele servers van de WMS leveren.	X	
6.	Beheer de virtuele servers, in overeenstemming met de beveiligingsrichtlijnen van het waterschap.		X
7.	Bewaak de hypervisors en hosts van de WMS op de beschikbaarheid en capaciteit van systeemgebeurtenissen.	X	
8.	Waterschap op de hoogte stellen in geval van problemen.	X	
9.	Aanvragen voor nieuwe virtuele server(s) of wijzigingen in bestaande virtuele server(s) initiëren als standaard serviceverzoek.		X
10.	Alle standaard serviceaanvragen verwerken, in overeenstemming met de serviceniveaudoelen	X	
11.	Incidentbeheer uitvoeren op problemen die worden veroorzaakt door gebeurtenissen en/of waterschap.		X
12.	Wijzigingsbeheer uitvoeren voor alle wijzigingen die nodig zijn om de omgeving van de virtuele servers te onderhouden volgens de serviceniveaudoelen		X
13.	Gebruik role-based access voor productiesupport.		X

3. Beschikbaarheidsbeheer, omgeving van virtuele servers

Beschikbaarheidsbeheer van de omgeving van virtuele servers bestaat uit de taken die de beschikbaarheid en capaciteit van de virtuele servers van de WMS bewaken en beheren.

Leverancier zal voldoen aan de verantwoordelijkheden, zoals uiteengezet in de volgende tabel.

No.	Taak
1.	Activiteiten uitvoeren ter ondersteuning van de levering, in overeenstemming met de doelstellingen voor het serviceniveau voor beschikbaarheid.
2.	Zorg voor geautomatiseerde beschikbaarheids- en capaciteitsbewaking van de hypervisors, hosts en virtuele servers van de WMS.
3.	Monitoren om incidenten te voorkomen en op te sporen.
4.	Proactief beheer om ongeplande uitval mogelijk te verminderen.
5.	Activeer het incidentbeheerproces automatisch, indien nodig.
6.	Op rollen gebaseerde toegang gebruiken voor productieondersteuning.

4.2.5 Operating Systeem

Microsoft Windows Server

Specifiek voor de Microsoft Windows Server-omgeving is het volgende:

- Antivirusbescherming
- Softwarelicentie voor virusbeschermingsbeheer.
- Inclusief softwarelicenties voor de volgende Microsoft-producten: Windows Server (inclusief terminalserver) en monitoring product.
- WMS monitoring/rapportage voor beheer, patch update status, virus status.

WMS Windows server patchbeleid is gebaseerd op het Microsoftpatchbeleid. Wanneer Microsoft nieuwe patches voor beveiligingsbesturingssysteem uitbrengt, worden deze geanalyseerd en worden relevante patches voor het besturingssysteem geïmplementeerd in het onderhoudsvenster. Relevante patches van andere leveranciers binnen het WMS-bereik worden geanalyseerd, voorbereid voor distributie en gedistribueerd in het patchvenster naar alle instanties van de bijbehorende versie en release van het besturingssysteem. De waterschappen worden geïnformeerd welke wijzigingen op welk moment worden doorgevoerd. Tijdens het onderhoudsvenster wordt de server opnieuw opgestart wanneer dit nodig is voor de implementatie van deze patches.

Ook als een specifieke virtuele machine een probleem ondervindt en de hoofdoorzaak permanent kan worden opgelost door een patch toe te passen, wordt een dergelijke patch toegepast op de betrokken servers.

Om ervoor te zorgen dat de omgeving veilig blijft, wordt tooling gebruikt om de status van patches en servicepacks voor het basis besturingssysteem te controleren en te rapporteren. Deze programma's gebruiken richtlijnen voor het bijwerken van fysieke servers en virtuele machines.

Linux Server

Specifiek voor de Linux-omgeving zijn de volgende items:

- Installatie- en patchfunctionaliteit in de WMS-beheeromgeving
- Monitoring server
- SSH stepping stone server
- Antivirussoftware

4.2.6 Patchbeleid

Linux-leveranciers geven regelmatig een samenhangende set patches uit. De installatie van een dergelijke coherente set valt onder dit serviceonderdeel en wordt uitgevoerd tijdens het onderhoudsvenster.

Relevante patches worden geanalyseerd, voorbereid voor distributie en vervolgens gedistribueerd en geïnstalleerd naar alle besturingssystemen van de bijbehorende versie en release van het besturingssysteem. De waterschappen worden geïnformeerd welke wijzigingen op welk moment worden doorgevoerd. Softwaredistributie van fixes en patches wordt gecontroleerd door het change managementproces.

Als een specifiek systeem een probleem ondervindt en de hoofdoorzaak permanent kan worden opgelost door een patch toe te passen, wordt een dergelijke patch toegepast op het betreffende systeem.

4.2.7 Backup

Backup and Restore is een back-up en herstel op VM/bestandsniveau, uitgevoerd op virtuele machines.

Back-up op bestandsniveau omvat de partitie van het besturingssysteem en alle gegevenspartities en bestaat uit het plannen, uitvoeren en verifiëren van routinematige back-ups. In het geval van een systeemstoring wordt de functionaliteit van het besturingssysteem en de gegevenspartities hersteld vanaf back-upmedia.

Back-up op bestandsniveau maakt geen back-up van geopende bestanden, wat geen beperking is om de functionaliteit van het besturingssysteem te herstellen. Als een toepassing een back-up van geopende bestanden vereist, heeft deze een extra toepassings back-up nodig via extra open-bestandsagents. Applicatie Backup and Restore is niet inbegrepen in deze service, maar kan worden gerealiseerd via dezelfde back-up-infrastructuur.

Er is een standaard bewaartermijn van de back-up op bestandsniveau. De back-up is samengesteld uit een regelmatige volledige back-up en tussentijdse incrementele back-ups.

Op verzoek zal WMS het herstel starten na ontvangst van een bevestiging van het te herstellen punt. Operatie voert regelmatig controles uit van de back-up-procedures en back-up-resultaten.

Op specifiek verzoek van een waterschap is het mogelijk om te definiëren dat een systeem geen back-up heeft.

4.2.8 Disaster recovery management

Disaster Recovery (DR)-beheer biedt functionaliteit voor het herstel van virtuele servers in het geval dat een uitval door het waterschap wordt gemeld.

De beschikbaarheid van de door het waterschap zelf beheerde besturingssystemen of toepassingen (aangezien sommige mogelijk niet compatibel zijn met de gebruikte toolsets en/of mechanismen) valt buiten het bereik en wordt niet ondersteund door WMS.

Herstel van klantinhoud die wordt gehost op virtuele servers valt buiten het bereik en wordt niet ondersteund en moet door het waterschap worden gevalideerd.

Indien er geen back-up services worden afgenomen door het waterschap, draagt het waterschap de enige verantwoordelijkheid voor het zorgen voor een adequate back-up van de inhoud van de virtuele server.

Disaster recovery management moet deel uitmaken van het overkoepelende waterschap disaster recovery strategie.

Er zijn twee patronen van disaster recovery, active-active en active-passive.

- Bij active-active wordt de dienst vanuit twee locaties geleverd. Als een van de locaties uitvalt, is de dienst nog steeds beschikbaar op de andere locatie. De capaciteit is wel beperkt (gebruikelijk 70% van de totale behoefte).
- Bij active-passive wordt de dienst vanuit één locatie geleverd. Er is een tweede locatie beschikbaar die bij verstoringen geactiveerd wordt.

Het ondersteunen van beide patronen verhoogt de complexiteit, die juiste bij verstoringen tot (menselijke) fouten zal leiden. Om deze reden is er gekozen om alleen active-active te ondersteunen, ook omdat dit voor business kritische applicaties het beste is én de eenvoudigste draaiboeken met zich meebrengt.

Active-active disaster recovery-operaties bestaan uit beheeractiviteiten die door Leverancier en waterschap moeten worden uitgevoerd in normale activiteiten van de WMS-infrastructuur.

Alle virtuele servers die worden uitgevoerd op een stretched cluster over twee fysieke sites, handelen alsof ze één zijn. Deze worden dan beschermd door HA en zullen als één geheel optreden. In het geval van een sitefout staan de gegevens al op de andere site en kunnen ze opnieuw worden opgestart als normaal "d.w.z. HA-gebeurtenis opnieuw opstarten".

Waterschap en Leverancier zullen zich houden aan de verantwoordelijkheden, zoals uiteengezet in de volgende tabel waarin de details van het logische herstelproces worden beschreven.

OPMERKING: Dit is een bedrijfsherstelplan.

No.	Taak	Leverancier	Waterschap
1.	Besluiten om het herstelplan uit te voeren na een ramp.	X	
2.	Toestemming om het herstelplan uit te voeren.		X
3.	Het herstelplan uitvoeren.	X	
4.	Geef contactgegevens van het waterschap op voor noodherstel.		X
5.	Werk de processen en de contactgegevens van het klantcontactpunt jaarlijks bij.	X	
6.	Virtuele servers testen die in aanmerking komen voor Disaster Recovery (DR).	X	
7.	Reserveer servercapaciteit in het aangrenzende datacenter infrastructuuronderdeel voor DR-geschikte virtuele servers.	X	
8.	Consolidatie storage van DR-aangewezen virtuele servers naar de gerepliceerde storage.	X	
9.	Onderhouden Customer recovery plan.		X
10.	Aanvraag veranderingen aan het recovery plan.		X
11.	Uitvoeren verandering aan het recovery plan door middel van het change proces.	X	
12.	Monitor de DR-infrastructuur.	X	
13.	Test en evaluatie van recovery plan	X	X

4.2.9 Container management

WMS maakt gebruik van Kubernetes en/of Docker als container technologie binnen de container infrastructuur functionaliteit. Hierdoor kan WMS-compatibele/gevalideerde containertechnologie worden gebruikt om containergebaseerde hosting en orchestratie te bieden.

Container Service bestaat uit de volgende onderdelen:

1. Ondersteuning voor containeromgevingen

Waterschap en Leverancier zullen voldoen aan de verantwoordelijkheden, zoals uiteengezet in de volgende tabel.

No.	Task	Leverancier	Waterschap
1.	Beheer de hypervisors die de virtuele servers leveren.	X	
2.	Beheer de virtuele servers, in overeenstemming met de beveiligingsrichtlijnen van de WMS.	X	
3.	Beheer de virtuele servers, in overeenstemming met de beveiligingsrichtlijnen van het waterschap.		X
4.	Containerbeheer servers en containercluster-VM's registreren in de WMS-beheerstack.	X	
5.	Het containercluster en beheeraccount voor het waterschap maken.	X	
6.	Gehoste workloads in containers beheren.		X
7.	Beheeraccounts en accountgegevens binnen het containercluster.		X
8.	Bewaak de hypervisors en hosts op systeem gebeurtenissen, beschikbaarheid en capaciteit, volgens het proces.	X	
9.	Waterschap op de hoogte brengen van eventuele problemen.	X	
10.	Aanvragen voor nieuwe containerclusters of wijzigingen in bestaande containerclusters initiëren als een standaard serviceaanvraag.		X
11.	Alle standaard serviceaanvragen verwerken, in overeenstemming met de serviceniveaudoelen	X	
12.	Incidentbeheer uitvoeren op problemen die worden veroorzaakt door gebeurtenissen of de Klant, zoals beschreven door het proces.	X	
13.	Wijzigingsbeheer uitvoeren voor alle wijzigingen die nodig zijn om de containerclusters te onderhouden volgens de serviceniveaudoelen.	X	
14.	Beheer de containerworkloads, in overeenstemming met de beveiligingsrichtlijnen van het waterschap.		X

2. Beschikbaarheidsbeheer van containeromgevingen

Beschikbaarheidsbeheer, de omgeving van virtuele servers bestaat uit de taken om de beschikbaarheid en capaciteit van de virtuele servers van de WMS te bewaken en te beheren. Waterschap en Leverancier zullen voldoen aan de verantwoordelijkheden, zoals uiteengezet in de volgende tabel.

No.	Task	Leverancier	Waterschap
1.	Activiteiten uitvoeren ter ondersteuning van de levering, in overeenstemming met de doelstellingen voor het beschikbaarheidsserviceniveau	X	
2.	Zorg voor geautomatiseerde beschikbaarheid en capaciteitsbewaking van de hypervisors en op containers gebaseerde virtuele servers.	X	
3.	Behoud de beschikbaarheid en capaciteitsbewaking van de containerclusters.		X
4.	Monitoren om incidenten met containerinfrastructuur te voorkomen en te detecteren.	X	
5.	Proactief beheer om ongeplande uitval mogelijk te verminderen.	X	
6.	Activeer het incidentbeheerproces automatisch, indien nodig.	X	

4.3 WMS - infrastructuur

Naast de services die worden geleverd in de sectie WMS-core services, bestaat de WMS-infrastructuur uit de volgende aanvullende componenten:

1. Beheer van virtuele opslag
2. Virtueel datacenter LAN
3. Virtuele firewall services

4.3.1 Beheer van virtuele opslag

Virtuele opslag biedt opslagcapaciteit en opslagtoegang tot de datastores, waar alle VM's zich bevinden. Waterschap-VM's die via WMS zijn ingericht, gebruiken opslag uit deze datastore.

Virtuele opslag is gebaseerd op interne schijven, gedistribueerd in een clusteromgeving en beheerd door software, waardoor de volgende mogelijkheden mogelijk zijn:

- Levering van opslagdiensten
- Redundantie om de beschikbaarheid te verhogen
- Op beleid gebaseerde opslag voor flexibele IOPS-inrichting (input/output operations per second; zie onderstaande tabel)

Server hardware en interne opslag lay-out is gedefinieerd in de WMS-architectuur ontwerp.

Leverancier is verantwoordelijk voor het implementeren en configureren van opslag op een waterschap-WMS. Virtuele opslag bestaat uit de volgende onderdelen:

- Productie ondersteuning
- Gebruik van interne opslag

Opslag klasses

1. Standaard opslagklassen in WMS zijn gebaseerd op IOPS-beperkingen die op storage-niveau zijn geïmplementeerd.
2. WMS-opslag wordt 100% gedeeld en garandeert geen IOPS per VM / object / waterschap.

Alle opslag gebeurt op basis van RAID5-technologie. Er worden enkele (3?) opslagklasses ondersteund.

Productiesupport

Productie ondersteuning:

- Biedt een reeks productieondersteunende activiteiten voor het huishouden van de servers, opslag en back-up infrastructuur
- Automatiseert operationele activiteiten
- Controleert of de processen en automatisering werken zoals bedoeld en er is regelmatig onderhoud.

Leverancier zal zich houden aan de verantwoordelijkheden, zoals uiteengezet in de volgende tabel.

No.	Task
1.	Beheer de opslag- en serverhardware en -software.
2.	Opslagbeheer uitvoeren volgens het beleid van de leverancier en beveiligingsrichtlijnen.
3	Zorg voor infrastructuur-, product- en leveranciersbeheer.
4	Als software vereist is op de server, moeten er gerelateerde softwareondersteuning bieden.
5	Onderhoudswerkzaamheden uitvoeren binnen de afgesproken onderhoudsvensters.
6	Zorg voor het vereiste onderhoud op een commercieel redelijke uitvoerbare basis.

4.3.2 Virtueel datacenter LAN

Virtueel datacenter local area network (LAN) biedt LAN-services, gehost in de datacenterlocaties van de leverancier. Sdn-principes (Software-defined networking) worden toegepast om netwerkservices los te koppelen van het onderliggende fysieke netwerk.

Virtueel datacenter LAN bestaat uit de volgende componenten:

1. Softwaregedefinieerde netwerken – core

   Biedt virtualisatietechnologie om de netwerkservices los te koppelen van het onderliggende fysieke netwerk. Waterschap en Leverancier zullen de verantwoordelijkheden, zoals uiteengezet in de volgende tabel, naleven.

No.	Task	Leverancier	Waterschap
1.	Bedien en onderhoud het softwaregedefinieerde netwerkonderdeel in overeenstemming met de huidige normen van de leverancier.	X	
2.	Toevoegen/wijzigen/verwijderen logical switches.	X	
3.	Toevoegen/wijzigen/verwijderentransport zone(s).	X	
4.	Toevoegen/wijzigen/verwijderendistributed switches.	X	
5.	Toewijzen/registreren IP adressen/netwerken voor waterschap zone(s).	X	

No.	Task	Leverancier	Waterschap
6.	Leveren IP-adressen/netwerken voor waterschap zone(s).	X	X

2. Fysieke connectiviteit en verbinding met core datacenternetwerken

Fysieke connectiviteit biedt een volledig gerouteerd layer 3-netwerk over spine/leaf-architectuur, als het onderliggende fysieke netwerk volledig geleverd en beheerd door de leverancier inclusief de connectie naar de WMS

3. Load balancing

Load balancing biedt netwerk taakverdeling voor webservices en toepassingen. Het bestaat uit lokale load balancing voor applicaties binnen de hosting WMS-omgeving.

Leverancier zal voldoen aan de verantwoordelijkheden, zoals uiteengezet in de volgende tabel.

No.	Task
1.	Operatie en onderhouden van de basis load balancing functies van de virtueel datacenter netwerkservice.
2.	Toevoegen/wijzigen/verwijderen basis load balancing services.
3.	Definieer load balancing parameters/algorithms.

4. Verbinding met oudere netwerken

Verbinding met legacy-netwerken biedt de mogelijkheid om een verbinding te maken met legacy-infrastructuur via het bestaande WAN van een waterschap.

No.	Task	Leverancier	Waterschap
1.	Maak mogelijk en beheer de mogelijkheid om te verbinden naar legacy infrastructuur van een Waterschap bestaande WAN.	X	
2.	Toevoegen/wijzigen/verwijderen legacy netwerk connection(s) gebaseerd op gateways.	X	
3.	Geef gedetailleerde informatie over legacy netwerkinfrastructuur (bijv. IP-netwerken, WAN, enz.).		X
4.	Zorg voor de WAN-verbinding tussen het netwerk van waterschap en het datacenter van de leverancier.		X

4.3.3 Virtuele firewall services

Virtuele firewallservices bieden firewalloplossingen voor virtuele omgevingen.

…. Verder uitwerken ???

4.4 Service levels en service verzoeken

4.4.1 Service beschikbaarheid

Er zijn standaard afspraken over de servicebeschikbaarheid die geleverd wordt door het WMS-platform. Er is een standaard service window dat altijd geldt, maar daarnaast zijn er maintenance windows voor onderhoudswerkzaamheden.

4.4.2 Support beschikbaarheid

Ook de beschikbaarheid van support is gestandaardiseerd, met vaste tijden voor normaal support en voor prioriteitsmeldingen.

4.4.3 Service levels (aanpassen)

De verschillende prioriteiten van meldingen corresponderen met bijpassende TTR's (Time To Resolve). Van alle type meldingen is de bijbehorende prioriteit afgsproken.

4.4.4 Aanvullend service levels/KPIs

Aanvullende serviceniveaus en KPI's die bij deze service worden geleverd, zijn als volgt. Standaard wijzigingen en serviceverzoeken worden vooraf gedefinieerd en overeengekomen met het waterschap. Serviceniveaus worden automatisch gemeten vanaf de duur van het openen/sluiten van het ticket.

4.4.5 Standard Rapporten

Standaard maakt WMS gebruik van de beschikbare oplossingen voor zijn live rapportagemogelijkheden voor capaciteit, status, enz., beschikbaar voor leverancier of waterschap. De volgende standaardrapporten worden bij deze service geleverd.

Report name	Description	Reporting period
Capacity and utilization	▸ Capacity allocation overview ▸ Cluster utilization ▸ Datastore utilization ▸ Heavy hitter VMS ▸ Host utilization ▸ Utilization overview ▸ VM utilization ▸ Virtuele storage capacity overview	Monthly
Configuration and compliance	▸ Cluster configuration ▸ Distributed switch configuration ▸ Host configuration ▸ VM configuration ▸ Hypervisor hardening compliance	Monthly
Operational reports	▸ Datastore usage overview ▸ Host usage overview ▸ Migrate to virtual storage ▸ Operations overview ▸ Virtual storage operations overview ▸ Mp statistics ▸ Self cluster statistics ▸ Self health ▸ Self performance details ▸ Self services communications ▸ Self services summary ▸ Self troubleshooting ▸ Cloud management adapter details	Monthly
Optimization	▸ Assess cost ▸ Optimization history ▸ Optimize performance	Monthly
Performance troubleshooting	▸ Troubleshoot a cluster ▸ Troubleshoot a datastore ▸ Troubleshoot a host ▸ Troubleshoot a VM	Monthly

Report name	Description	Reporting period
	▸ Troubleshoot virtual storage ▸ Troubleshoot with logs	
Assessment	▸ Hybrid cloud assessment ▸ Hypervisor optimization assessment	Monthly
Automation	▸ Application overview ▸ Environment overview ▸ Resource consumption overview ▸ Top-n	Monthly